TLE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,903	01/10/2001	Luis M. Ortiz	K1033	8298

7590 03/07/2006

ORTIZ & LOPEZ, PLLC
Patent Attorney
P. O.4484
Albuquerque,, NM 87196-4484

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/757,903	ORTIZ, LUIS M.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-23,25-34 and 36-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-23,25-34 and 36-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the Pre-Brief Appeal decision to re-open prosecution. Claims 1-12, 14-23, 25-34, and 36-44 are currently being considered.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6,8-12, 14,16-23, 25-28,30-34,36, and 38-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Abrahams (U.S. Patent No. 6,944,773).

Regarding claim 1, Abrahams discloses:

A method for biometrically securing access to an electronic system, said method comprising the steps of:

using a computer network to obtain a user profile from a server (column 2 lines 55-62), wherein a computer network is used to access a database storing fingerprints;

prompting a user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from said user profile containing biometric attributes of said user (column 3 lines 27-50); and

permitting said user to perform a user-desired activity, if at least one biometric attribute input by said user to said biometric user interface associated with said

electronic system matches said at least one biometric attribute randomly selected from said user profile (column 3 lines 27-50).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said computer network is a secure computer network (column 2 lines 55-62, column 6 lines 50-56), wherein secure financial transactions are performed.

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said user profile is stored in a biometric broker (column 2 lines 59-61), wherein the database stores user profiles and associated fingerprints.

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 further comprising the steps of:

obtaining at least one biometric attribute from said user for compilation in said user profile (column 3 lines 45-50);

compiling said user profile (column 3 lines 45-50); and

storing said user profile in said server accessible by at least one biometric user interface associated with said electronic system (column 2 lines 55-63, column 3 lines 45-50).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 4 further comprising the step of:

permitting said user to modify said user profile, in response to approval of a request by said user (column 1 line 47 – column 2 line 8).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile (column 5 lines 30-40).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said electronic system comprises at least one wireless device that operates with a wireless network (column 2 lines 63-67).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said electronic system comprises at least one computer workstation operable over an associated network (column 2 lines 63-67).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said electronic system comprises an automated teller machine (column 6 lines 50-56).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said electronic system comprises a secured entry system to a secured environment (column 6 lines 50-56).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said electronic system comprises a wireless network (column 2 lines 63-67).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said electronic system comprises a wireless device (column 2 lines 63-67).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said user-desired activity comprises a financial transaction (column 6 lines 50-56).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said user-desired activity comprises an ATM transaction (column 6 lines 50-56).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said user-desired activity comprises access to a secure area (column 6 lines 50-56).

Claim 19 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said user-desired activity comprises access to data from said electronic system (column 6 lines 50-56).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 wherein said user desired activity comprises execution of a mechanical activity (column 6 lines 50-56).

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Abrahams discloses:

The method of claim 1 further comprising the steps of:

initiating access to said electronic system utilizing only one biometric attribute to said electronic system (column 5 lines 35-40), wherein the random number of fingerprints can be set to one.

Regarding claim 22, Abrahams discloses:

A method for biometrically securing access to an electronic system, said method comprising the steps of:

using a computer network to obtain a user profile from a server (column 2 lines 55-62), wherein a computer network is used to access a database storing fingerprints;

prompting a user to input to a biometric user interface associated with said electronic system at least two biometric attributes randomly selected from said user profile containing biometric attributes of said user (column 3 lines 27-50, column 5 lines 30-54);

permitting said user to perform a user-desired activity, if biometric attributes input by said user to said biometric user interface associated with said electronic system matches said at least two biometric attribute randomly selected from said user profile (column 3 lines 27-50, column 6 lines 50-56).

Regarding claim 23, Abrahams discloses:

A system for biometrically securing access to an electronic system, said system comprising:

a server connected to a computer network adapted to store at least one user profile, and capable of allowing at least one biometric user interface associated with said electronic system also connected to said computer network to access said at least one user profile (column 2 lines 55-62), wherein a computer network is used to access a database storing fingerprints;

biometric user interface associated with said electronic system and connected to said computer network that accesses a user profile stored on said server that contains biometric attributes of said user and that prompts said user to input to said electronic system at least one biometric attribute randomly selected from said user profile (column 3 lines 27-50, column 5 lines 30-54); and

an electronic system for permitting said user to perform a user-desired activity, if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile (column 3 lines 27-50, column 6 lines 50-56).

Claim 25 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user profile is accessible from a biometric broker via a secure network connection (column 2 lines 59-61), wherein the database stores user profiles and associated fingerprints.

Claim 26 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein:

at least one biometric attribute is obtained from said user for compilation in said user profile (column 3 lines 45-50).

Claim 27 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user is permitted to modify said user profile, in response to approval of a request by said user (column 1 line 47 – column 2 line 8).

Claim 28 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 further comprising:

module for comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile (column 5 lines 30-40).

Claim 30 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said electronic system comprises at least one wireless device that operates with a wireless network (column 2 lines 63-67).

Claim 31 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said electronic system comprises at least one computer workstation over said computer network (column 2 lines 63-67).

Claim 32 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said electronic system comprises an automated teller machine (column 6 lines 50-56).

Claim 33 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said electronic system comprises a secure entry system to a secured environment (column 6 lines 50-56).

Claim 34 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said computer network comprises a wireless network (column 2 lines 63-67).

Claim 36 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said electronic system comprises a wireless device (column 2 lines 63-67).

Claim 38 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user-desired activity comprises a financial transaction (column 6 lines 50-56).

Claim 39 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user-desired activity comprises an ATM transaction (column 6 lines 50-56).

Claim 40 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user-desired activity comprises access to a secure area (column 6 lines 50-56).

Claim 41 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user-desired activity comprises access to data from said electronic system (column 6 lines 50-56).

Claim 42 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein said user-desired activity comprises execution of a mechanical activity (column 6 lines 50-56).

Claim 43 is rejected as applied above in rejecting claim 23. Furthermore, Abrahams discloses:

The system of claim 23 wherein access to said electronic system is initiated utilizing only one biometric attribute input to said biometric user interface associated with said electronic system (column 5 lines 35-40), wherein the random number of fingerprints can be set to one.

Regarding claim 44, Abrahams discloses:

A system for biometrically securing access to an electronic system, said system comprising:

a server connected to a computer network that is adapted to store at least one user profile and is capable of allowing at least one biometric user interface associated with said electronic system and connected to said computer network to access said at least one user profile (column 2 lines 55-62), wherein a computer network is used to access a database storing fingerprints;

a biometric user interface associated with said electronic system and connected to said computer network that accesses a user profile stored on said server that contains biometric attributes of said user and that prompts said user to input to said biometric user interface at least two biometric attributes randomly selected from said user profile (column 3 lines 27-50, column 5 lines 30-54); and

an electronic system for permitting said user to perform a user-desired activity, if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile (column 3 lines 27-50, column 6 lines 50-56).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 7,15,29, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abrahams (U.S. Patent 6,944,773) in view of Price-Francis (U.S. Patent 5,815,252).

Claim 7 is rejected as applied above in rejecting claim 1. Abrahams does not explicitly disclose subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. However, Price-Francis discloses subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. Abrahams and Price-Francis are analogous arts in that both use fingerprints to authenticate a user before allowing the user to perform a secured activity. It would have been obvious to modify the system of Abrahams of authenticating users using random fingerprints, with the system of Price-Francis "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 15 is rejected as applied above in rejecting claim 1. Abrahams does not explicitly disclose subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user

profile. However, Price-Francis discloses subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. Abrahams and Price-Francis are analogous arts in that both use fingerprints to authenticate a user before allowing the user to perform a secured activity. It would have been obvious to modify the system of Abrahams of authenticating users using random fingerprints, with the system of Price-Francis "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 29 is rejected as applied above in rejecting claim 28. Abrahams does not explicitly disclose subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. However, Price-Francis discloses subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. Abrahams and Price-Francis are analogous arts in that both use fingerprints to authenticate a user before allowing the user to perform a secured activity. It would have been obvious to modify the system of Abrahams of authenticating users using random fingerprints, with the system of Price-Francis "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors,

such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 37 is rejected as applied above in rejecting claim 23. Abrahams does not explicitly disclose subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. However, Price-Francis discloses subsequently prompting a user to input another biometric input if at least one previously input biometric does not match the randomly selected biometric in the user profile. Abrahams and Price-Francis are analogous arts in that both use fingerprints to authenticate a user before allowing the user to perform a secured activity. It would have been obvious to modify the system of Abrahams of authenticating users using random fingerprints, with the system of Price-Francis "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
03/02/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100